AMENDMENTS TO THE CLAIMS

1. **(Currently Amended)** An encrypted communication system comprising a first device and a second device, wherein

the first device (i) encrypts a first key using a public key of the second device to generate first encrypted data, and transmits the first encrypted data to the second device, (ii) receives second encrypted data from the second device, the second encrypted data being generated by encrypting a third key of the second device using a public key of the first device at the second device, and decrypts the second encrypted data using a secret key of the first device to obtain a second key, and (iii) generates, based on the first and second keys, a first encryption key for use in communication with the second device,

the second device (i) encrypts the third key using the public key of the first device to generate the second encrypted data, and transmits the second encrypted data to the first device, (ii) receives the first encrypted data from the first device, and decrypts the first encrypted data using a secret key of the second device to obtain a fourth key, and (iii) generates, based on the third and fourth keys, a second encryption key for use in communication with the first device, and

the first and second devices perform encrypted communication using the first and second encryption ~~keys~~keys,

wherein the first device concatenates the first and second keys to generate concatenated data, calculates a hash value for the concatenated data, generates the first encryption key and a first hash key based on the hash value for the concatenated data, calculates using the first hash key a first hash value for the first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device, the first encryption key being distinct from the first hash key,

~~wherein the first device generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate~~

~~encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device, the first encryption key being distinct from the first hash key~~,

wherein the second device generates the second encryption key and a second hash key based on the third and fourth keys, receives from the ~~communication~~ first device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data to generate decrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the decrypted first transmission data is not tampered with when the received first hash value matched the calculated second hash value, the second encryption key being distinct from the second hash key.

2. **(Currently Amended)** A communication device for performing encrypted communication with another device using a shared key, comprising:

a data generation unit operable to encrypt a first key using a public key that corresponds to a secret key held by the other device to generate first encrypted key data, and transmit the first encrypted key data to the other device;

a decryption unit operable to receive, from the other device, second encrypted key data, the other device generating the second encrypted key data by encrypting a third key using a public key of the communication device, and decrypt the second encrypted key data using a secret key of the communication device to obtain a second key;

a key generation unit operable to generate a first encryption key based on the first and second keys; and

a communication unit operable to perform encrypted communication with the other device using the first encryption key, the other device receiving from the communication device the first encrypted key data, decrypting the first encrypted key data using a secret key of the other device to obtain a fourth key, and generating a second encryption key corresponding to the first encryption key based on the third and fourth keys,

wherein the key generation unit further generates the first encryption key and a first hash

key based on the first and second keys, the first encryption key being distinct from the first hash key,

the communication device includes:

a calculation unit operable to calculate, using the first hash key, a first hash value for transmission data; and

an encryption unit operable to encrypt the transmission data using the first encryption key to generate encrypted transmission data, and

the communication unit further transmits the first hash value and the encrypted transmission data to the other device, and

wherein the communication device includes an authentication unit operable to:

receive from the other device a second hash value for second transmission data and encrypted second transmission data, the other device generates the second encryption key and a second hash key based on the third and fourth keys, calculates using the second hash key the second hash value for the second transmission data, encrypts the second transmission data using the second encryption key to generate encrypted second transmission data, and transmits the second hash value and the encrypted second transmission data to the communication device, the second encryption key being distinct from the second hash key;

decrypt the encrypted second transmission data to generate decrypted second transmission data using the first encryption key;

calculate using the first hash key a second hash value for the decrypted second transmission data; and

determine that the decrypted second transmission data is not tampered with when the received second hash value matches the calculated second hash value, and

wherein the communication device concatenates the first and second keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the first encryption key and the first hash key based on the hash value for the concatenated data.

3-4. **(Canceled)**

5. **(Previously Presented)** The communication device of claim 2, wherein the key generation unit performs an exclusive OR operation using the first and second keys, and generates the first encryption key and the first hash key based on a result of the operation.

6-9. **(Canceled)**

10. **(Previously Presented)** The communication device of claim 2, wherein

the data generation unit encrypts the first key based on a key encapsulation mechanism to generate the first encrypted key data, and

the decryption unit decrypts the second encrypted key data based on a key decryption mechanism to obtain the second key.

11. **(Currently Amended)** A method used by a communication device that performs encrypted communication with another device using a shared key, comprising:

encrypting a first key using a public key that corresponds to a secret key held by the other device to generate first encrypted key data;

transmitting the first encrypted key data to the other device;

receiving, from the other device, second encrypted key data, the other device generating the second encrypted key data by encrypting a third key using a public key of the communication device;

decrypting the second encrypted key data using a secret key of the communication device to obtain a second key;

generating a first encryption key and a first hash key based on the first and second keys, the first encryption key being distinct from the first hash key;

performing encrypted communication with the other device using the first encryption key, the other device receiving from the communication device the first encrypted key data, decrypting the first encrypted key data using a secret key of the other device to obtain a fourth

key, and generating a second encryption key corresponding to the first encryption key based on the third and fourth keys,

calculating using the first hash key a first hash value for transmission data;

encrypt the transmission data using the first encryption key to generate encrypted transmission data; and

transmitting the first hash value and the encrypted transmission data to the other device;

receiving from the other device a second transmission data and encrypted second transmission data, the other device generating the second encryption key and a second hash key based on the third and fourth keys, calculating using the second hash key the second hash value for the second transmission data, encrypting the second transmission data using the second encryption key to generate encrypted second transmission data, and transmitting the second hash value and the encrypted second transmission data to the communication device, the second encryption key being distinct from the second hash key;

decrypting the encrypted second transmission data to generate decrypted second transmission data using the first encryption key;

calculating using the first hash key a second hash value for the decrypted second transmission data; and

determine that the decrypted second transmission data is not tampered with when the received second hash value matches the calculated second hash value, and

wherein the communication device concatenates the first and second keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the first encryption key and the first hash key based on the hash value for the concatenated data.

12. **(Currently Amended)** A computer program recorded on a computer-readable medium, the computer program being used by a communication device that performs encrypted communication with another device using a shared key, the computer program causing a computer to execute:

encrypting a first key using a public key that corresponds to a secret key held by the other

device to generate first encrypted key data;

transmitting the first encrypted key data to the other device;

receiving, from the other device, second encrypted key data, the other device generating the second encrypted key data by encrypting a third key using a public key of the communication device;

decrypting the second encrypted key data using a secret key of the communication device to obtain a second key;

generating a first encryption key and a first hash key based on the first and second keys, the first encryption key being distinct from the first hash key;

performing encrypted communication with the other device using the first encryption key, the other device receiving from the communication device the first encrypted key data, decrypting the first encrypted key data using a secret key of the other device to obtain a fourth key, and generating a second encryption key corresponding to the first encryption key based on the third and fourth keys,

calculating using the first hash key a first hash value for transmission data;

encrypting the transmission data using the first encryption key to generate encrypted transmission data; and

transmitting the first hash value and the encrypted transmission data to the other device;

receiving from the other device a second hash value for second transmission data and encrypted second transmission data, the other device generating the second encryption key and a second hash key based on the third and fourth keys, calculating using the second hash key the second hash value for the second transmission data, encrypting the second transmission data using the second encryption key to generate encrypted second transmission data, and transmitting the second hash value and the encrypted second transmission data to the communication device, the second encryption key being distinct from the second hash key;

decrypting the encrypted second transmission data to generate decrypted second transmission data using the first encryption key;

calculating using the first hash key a second hash value for the decrypted second transmission data; and

determining that the decrypted second transmission data is not tampered with when the received second hash value matches the calculated second hash value and

wherein the communication device concatenates the first and second keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the first encryption key and the first hash key based on the hash value for the concatenated data.

13. **(Canceled)**

14. **(New)** The encrypted communication system of Claim 1, wherein

the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys.

15. (**New)** The communication device of Claim 2, wherein

the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys.

16. **(New)** The method of Claim 11, wherein

the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys.

17. **(New)** The computer program of Claim 12, wherein

the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys.